

ARS □ CSREES □ ERS □ NASS

Policies and Procedures

Title: Electronic Information and Systems Security

Number: 3200

Date: 9/30/94

Originating Office: Economics Management Staff

This Replaces: 1411 dated 5/1/86

Distribution: EMS only

This P&P states the policy, duties, and minimum program requirements for the security of EMS's electronic information and systems.

Table Of Contents

1.	Introduction	3
2.	Security Plan	3
	Basic Plan	3
	Security Reviews and Risk Analyses	3
	Contingency Plan	4
3.	Security Systems	4
4.	Security of Electronic Information	4
	Creating and Safeguarding Passwords	4
	Safeguarding Sensitive Data	4
	Safeguarding Privacy Act Records	5
	Access to Information Systems	5
	Backup	5
	Virus Testing	6
5.	Physical Security	6
	Theft	6
	Damage	6
6.	Copyright Protection	6
7.	Records Management	7
8.	Training Program	7
	Summary of Responsibilities	7
	Glossary	10

1. Introduction

EMS establishes and maintains security controls for electronic information systems and related hardware, software, and data communications equipment. To achieve such security, the Director of EMS appoints a security officer (SO) and qualified individual(s) to perform the Agency's security functions. The Chief of EMS's Systems Automation Branch (SAB) and the SO develop, implement, and maintain an effective security program to insure confidentiality, integrity, and availability of information for authorized/appropriate users.

2. Security Plan

Basic Plan

The basic plan documents the necessary security measures needed for electronic data, computer hardware, software, and related equipment. The SO updates the plan annually and submits it through the IRM Committee for final submission to the Departmental Security Officer in the Office of Information Resources Management (OIRM). The annual update specifies actions to be taken that year. At a minimum, the plan includes physical requirements to prevent theft or damage (see Chapter 5 of this P&P) and explains how the Agency will protect against:

- data loss or modification
- disclosure of confidential information
- unauthorized use of information resource assets (data, programs, hardware, software, passwords, account numbers, etc.)
- decreased operational reliability of hardware, software, data communications, and computer systems applications
- asset loss (hardware, software, supplies, programs, data, etc.)

Security Reviews and Risk Analyses

The SO develops and implements a plan to conduct and document yearly physical security reviews and risk analyses. Reviews include surveys of the backup or contingency plans as described below. Risk

Analysis factors the impact of an event against the potential frequency of the event to determine appropriate security measures. Security crises range from severe natural disasters such as fire and flood, to viruses on computers and inadvertent deletions of data.

Contingency Plan

Contingency planning covers all classes of business discontinuity, assigns responsibility for recovery and survival, and defines avoidance measures. The plan should include workable procedures for continuing to perform essential functions when information technology support is interrupted, as well as emergency procedures to be taken in the event of natural or civil disaster. The SO will work with the cognizant functional staff and management to develop these plans and procedures, as well as conduct annual reviews and tests to ensure their continued adequacy.

3. Security Systems

- All computer systems and applications used in EMS should comply with the following minimum security measures to ensure the integrity of the data and files, prevent unauthorized system access, and maintain control of the system programs and files:
- All multi-user systems should have built-in file and record-locking functions to ensure data integrity. In addition, user access rights should be limited and controlled via the network operating system or other appropriate means to prevent unauthorized access to system files and directories.
- The most recent version of computer application programs and related documentation should be safeguarded and properly labeled with version numbers and dates.
- New employees and contractors should be informed of and adhere to Agency electronic information and systems security policies.

4. Security of Electronic Information

Creating and Safeguarding Passwords

To ensure that employees access only data for which they are authorized, all sensitive data must be password protected or retained in a secure place. To prevent unauthorized access, users accessing

data protected by passwords should log-off the system after use or when leaving their workstations for an extended period of time. Furthermore, employees must protect against unauthorized disclosure of passwords, account numbers, access codes, and other means of access to data systems. Passwords should not be disclosed to fellow employees, nor recorded in a location where they could be read by other employees.

Safeguarding Sensitive Data

After assessing the sensitivity of systems and data, the Chief of SAB develops adequate security for the operations of those systems. Employees should promptly report any suspected violations of security or irregularities in electronic information and systems security to the SO and to their own immediate supervisors. In the event of a security breach in which criminal action or significant loss is reported or suspected, the SO will report the breach to OIRM and the Office of Inspector General. The SO also will confer with the Director of EMS's Personnel Division to determine the appropriate disciplinary action.

Safeguarding Privacy Act Records

In compliance with the Privacy Act of 1974, the SO will work with the Privacy Act Officer and records custodians to develop procedures for safeguarding systems of records protected by the Privacy Act.

Access to Information Systems

The Director of EMS's Personnel Division develops and implements procedures for issuing and monitoring EMS personnel security clearances that are necessary for information access in accordance with Federal and Departmental regulations.

All employees who access information systems must have authorization from their supervisors. Supervisors should send written requests to the SO authorizing employee access to mainframe and LAN applications. The SO processes all requests for providing user access to mainframe and LAN applications.

Division directors or other designated officials must notify the SO when employees with mainframe and/or LAN access leave their divisions, or if changes in employee responsibilities require changes in security. Furthermore, division directors ensure that employees comply with procedures outlined in P&P 4296, "Check-Out of Separating Employees. "

Backup

Since power surges, hardware problems, human errors, and computer viruses can corrupt or erase data, employees should take the following steps:

- secure all data by creating a backup copy of data files at least weekly
- backup all critical data after any significant modification
- store backup copies of data in a secure location

The Chief of SAB ensures that all data stored on network file servers is backed up to secure storage media on a daily basis.

Virus Testing

To minimize the risk of losing data as a result of a computer virus, the Chief of SAB ensures that all workstations and file servers within EMS run memory-resident scanning software for virus detection, and that detected viruses are immediately cleaned from the infected equipment to prevent further infection.

Employees should have any new, third-party software programs that are not on manufacturers' diskettes scanned for computer viruses by the Technical Analysis and Support Section (TASS) prior to installation. This includes, but is not limited to, public domain software, shareware, copies of commercial software not on manufacturers' diskettes, and inhouse software.

5. Physical Security

Theft

All doors and first floor windows in rooms housing computers, terminals, printers, software diskettes, and peripheral equipment must be locked after working hours, or when left unattended for long periods of time. Only personnel who need to conduct official business may operate such equipment. Additionally, original copies of commercial software should be stored in a secured location.

Damage

Environment. Excessive dirt, particles, and clutter can damage or shorten the functional life of microcomputers and terminal equipment. Employees should not smoke, eat, or drink around any computer workstation. Furthermore, employees should keep equipment vents clear for adequate air

circulation.

Preventive Maintenance. The Chief of SAB conducts an annual preventive maintenance program for microcomputers within EMS, which includes cleaning and testing hard drives, floppy drives, monitors, and CPU's.

6. Copyright Protection

USDA strictly forbids violation of licensing agreements. Most software currently in use is copyrighted, with all rights reserved to the copyrighter. This means that any copying, selling, or distributing software—for other than archival or other such purposes specifically allowed in the agreement—is a crime. (For example: WordPerfect Corporation licensing allows for home use of its word processing products when used primarily for work purposes.) Willful violation of licensing agreements can result in civil damages of up to \$50,000 in addition to actual damages, plus criminal penalties of up to 1 year imprisonment and/or a \$10,000 fine. Any questions regarding licensing agreements should be raised with the SO.

7. Records Management

Prior to the development of software systems, the Chief of SAB consults with the Chief of EMS's Management Analysis Branch (MAB), who serves as EMS's Records Management Officer. All electronic systems of records must be evaluated and, if necessary, scheduled by the Records Office. MAB works with program officials, the SO, and the National Archives and Records Administration to define legal retention requirements for electronic records. Also, MAB works with program managers to transfer electronic records to permanent or long-term storage.

8. Training Program

In compliance with Departmental regulations and the Computer Security Act of 1987, the SO will develop a training program to promote an awareness of the need for strong electronic information and systems security as well as the potential dangers and risks to data and personnel. Once trained, employees should consider making improvements to their data systems' security and notify the SO accordingly.

Summary of Responsibilities

Director, EMS

- Appoints the Agency Security Officer.

IRM Committee

- Reviews and approves electronic information and systems security policies, standards, and recommendations from SAB.

Chief, SAB

- Jointly with the SO develops, implements, and maintains the EMS electronic information and systems security program.
- Safeguards the most recent version of network computer application programs and related documentation.
- Conducts an annual preventive maintenance program for microcomputers within EMS.
- Ensures that all workstations and file servers within EMS run memory-resident scanning software for computer virus detection.
- Ensures that any detected viruses are immediately cleaned from the infected equipment to prevent further infection.
- Provides guidance for the implementation and maintenance of adequate electronic information and systems security, including the backing up of data.
- Ensures that all data stored on network file servers is backed up to secure storage media on a daily basis.

Security Officer

- Jointly with Chief of SAB develops, implements, and maintains the EMS electronic information and systems security program.
- Determines the agency's requirements for electronic information and systems security.
- Develops and recommends security policies, procedures, and standards.
- Complies with requests from agency officials to provide or remove user access to mainframe and LAN applications.

- Plans and conducts periodic security reviews.
- Ensures that all procurement of computer hardware, software, and information technology services incorporate adequate security provisions.
- Develops and implements (with functional staff and management) backup and contingency procedures.
- Reports to OIRM and the Office of Inspector General any security breaches in which criminal action or significant loss is suspected.

Director, PD

- Develops and implements procedures for issuing and monitoring any security clearances for EMS personnel.
- Works with the SO to develop and implement procedures for safeguarding employee data.

Chief, MAB

- Helps establish, with the SO, program officials, and the National Archives and Records Administration, legal retention requirements for electronic records.
- Assists program managers in the transfer of electronic records to permanent or longterm storage.
- As Privacy Act Officer, identifies systems of records that are protected by the Privacy Act. Works with the SO and records custodians to develop adequate safeguards for those records.

Division Directors

- Notify the SO when employees with mainframe and/or LAN access leave their divisions, or if changes in responsibilities require changes in security.
- Ensure that new employees and contractors are informed of, and adhere to, Agency electronic information and systems security policies.
- Safeguard the most recent version of division-specific computer application programs and related documentation.

Supervisors

- Send written requests to the SO authorizing employee access to mainframe and LAN applications.

All Employees

Protect computer equipment, software, and data from theft and damage.

Contact TASS for virus scanning of any new, third-party software programs not on manufacturers' diskettes prior to installation. This includes public domain software, shareware, copies of commercial software not on manufacturers' diskettes, and in-house software.

Backup data on a regular basis.

Protect against unauthorized disclosure of passwords and other means of access to data systems.

Access only such data, programs, and files for which they are authorized.

Report promptly any violations of security or observed irregularities in electronic information and systems security to the SO and also to their own immediate supervisors.

Notify the SO of needed security improvements.

Comply with all of the above procedures when working at either assigned duty station or other Federal work sites.

Glossary

Hardware. All physical components of computers and computer peripherals. This includes monitors, hard drives, computer boards, printers, modems, etc.

Software. All programs stored on a hard drive, floppy disk, CD ROM and other electronic storage mediums. This includes computer application programs, commercial software, etc.

Computer Applications. Programs written in a commercial software computer language for the purpose of automating a specific activity or group of related activities.

Computer Virus. Software programs that attach themselves to executable programs, altering the operation of the computer, and usually destroying the computer's data.

IRM. Information Resource Management.

LAN. Local Area Network.

MAB. EMS's Management Analysis Branch.

OIRM. USDA's Office of Information Resources Management.

SAB. EMS's Systems Automation Branch.

Security Officer (SO). An employee, appointed by the EMS Director, responsible for the implementation and maintenance of the EMS Electronic Information and Systems Security Program.

Sensitive Data. Includes, but is not limited to, employee information covered by the Privacy Act of 1974 and confidential economic and financial information. (See 5 U.S.C. 552a and 7 CFR 0.735-20.)